



United Student Aid Funds, Inc.

Mailing Address:

P.O. Box 6028, Indianapolis, IN 46206-6028

Corporate Address:

30 South Meridian Street, Indianapolis, IN 46204-3503

317-849-6510 800-428-9250

www.usafunds.org

Supporting access to education

October 6, 2000

Secretary, Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: Gramm-Leach-Bliley Act Privacy Safeguards Rule, 16 C.F.R. Part 313 - Comment

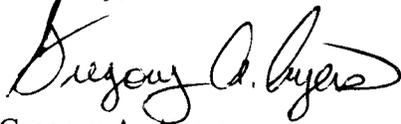
Dear Secretary:

Enclosed are comments in response to the September 7, 2000 advance notice of proposed rulemaking and request for comment regarding the Safeguards Rule pursuant to section 501(b) of the Gramm-Leach-Bliley Act (G-L-B Act). These comments are submitted on behalf of United Student Aid Funds, Inc. (USA Funds), the nation's largest guarantor of education loans made under the Federal Family Education Loan Program (FFELP). USA Funds is an Indiana-based nonprofit corporation that supports access to education by providing financial and other valued services to those who pursue, provide, or promote education. We are pleased to be afforded the opportunity to provide comments early in your regulatory process and hope that you will continue your dialogue with the financial community as you develop rules related to this complex statute.

USA Funds strongly supports safeguards to ensure the privacy of customer records and information. However, we caution against the inclusion of procedures and processes in the final regulations. The regulations will govern many different types of financial institutions, including many who participate in the FFELP. Such a diverse array of institutions has numerous procedures, processes, and systems already in place to support different regulatory and statutory requirements, some of which may provide direct or indirect compliance with certain requirements in section 501(b) of the G-L-B Act. For example, borrowers currently participating in the FFELP receive disclosures pursuant to the Privacy Act of 1974, the Right to Financial Privacy Act of 1978, and the Paperwork Reduction Act of 1995. Regulations accompanying these statutes have established "safeguards" or protection provisions to borrower information held by the regulated entities. Many of the current safeguards may be utilized to comply with any new regulations in support of the G-L-B ACT. However, these formats may not be used by other types of financial institutions. Each financial institution should be allowed to create and adjust internal procedures and processes as necessary in order to ensure compliance with all related statutes and rules, including the G-L-B ACT.

We appreciate the opportunity to provide comments on the advance notice of proposed rulemaking and hope that you will contact us with any questions regarding our concerns as we would welcome the opportunity to discuss further the context of our issues.

Sincerely,

A handwritten signature in black ink that reads "Gregory A. Ayers". The signature is fluid and cursive, with the first name being the most prominent.

Gregory A. Ayers
Vice President
Policy and Compliance
Gayers@usafunds.org
(317) 578-6649

GAA/sk
S:\Loanplcy\GREG\glbcover.doc

**Gramm-Leach-Bliley Act Privacy Safeguards Rule
16 CFR Part 313-Comment
Submitted by: USA Funds**



CITE: Section B. 1. Range of Information Subject to the Safeguards Rule

QUERY: What constitutes "customer records and information" under subsection (b), particularly in light of the reference to "customers' nonpublic personal information" in subsection (a)? [Section 501] Should the definition of "customer records and information" under the Safeguards Rule be similar to the definition of "nonpublic personal information" for customers under the Commissions' Privacy Rule?

RESPONSE: Information to which only the financial institution is privy should be considered "customer records and information" subject to the protections discussed in Section 501(a). Other, publicly available information should not be included in any confidentiality requirement. We believe that rules consistent with the Privacy Rule may be reasonable but would note that such rules serve best when developed simply and clearly without requiring burdensome verifications or cumbersome additional recordkeeping.

QUERY: Should the Safeguards Rule apply to "consumer" information maintained by a financial institution?

RESPONSE: If the term "consumer" is defined consistent with statute as an individual who obtains a financial product or service from the financial institution, then it is reasonable that the Safeguards Rule should apply to "consumer" information only to the extent that information meets the definition of nonpublic personal information.

QUERY: If the financial institution cannot accurately separate its customer records and information from its consumer records, should the Safeguards Rule require the financial institution to safeguard both types of records?

RESPONSE: The safeguards should only be applicable to records governed by the Act. While the financial institutional may choose to apply the safeguards to all records, there should be no requirement to apply the safeguards to any records other than the customer records and information.

CITE: Section B. 2. Range of Financial Institution Subject to the Safeguards Rule

QUERY: How should the Safeguards Rule apply when a financial institution discloses customer records and information to a financial institution that has no customer relationships or consumers?

RESPONSE: We believe the Act (Section 502(b)(2)) allows financial institutions to share nonpublic personal information with a third party if that third party enters into an agreement to maintain the confidentiality of the information. Thus both institutions are governed by statutory provisions already in place—as the original financial institution and one as a party to the contract ensuring confidentiality—and no additional regulation should be necessary.

QUERY: Should the Safeguards Rule require the originating financial institution to disclose its "customer records and information" subject to the agreement of a different financial institution that is receiving the information to comply with the Safeguards Rule in its handling of the information?

RESPONSE: Financial institutions should be bound to rules governing only those financial transactions occurring while the consumer/customer is the consumer/customer of the original financial institution and

only to those transactions which the institution itself performs. Any subsequent financial institution receiving customer records and information is, itself, governed by statute to develop appropriate safeguards.

CITE: Section C. Questions as to the other Aspects of the Commission's Safeguards Rule

QUERY: Should the Safeguards Rule take into account the need for financial institutions to keep pace with changing technology and other changes to their operational environment?

RESPONSE: The Safeguards Rule should not attempt to mandate operational or technological aspects of the financial institution's compliance with the regulation. Financial institutions already have sufficient financial and business incentives to remain abreast of technology and other applicable changes in the marketplace. The rule should, instead, set forth a viable standard for compliance and financial institutions should be permitted maximum flexibility to design complying systems based on their expansive knowledge of the market, technology, and their own systems and operational processes.

QUERY: Should the Safeguards Rule provide minimum procedures for a financial institution to follow and minimal levels of effectiveness that must be maintained?

RESPONSE: We recommend a rule similar to that of the SEC which provides institutions latitude to develop their own "reasonably designed" policies and procedures to achieve those standards. We reiterate that financial institutions have sufficient market incentive to develop complying processes that are efficient and effective.

QUERY: Are there any current guidelines in place (e.g., private standards, association rules) that may assist in development of safeguards standards for financial institutions subject to FTC jurisdiction?

RESPONSE: Currently, borrowers participating in the FFELP receive disclosures pursuant to the Privacy Act of 1974, the Right to Financial Privacy Act of 1978, and the Paperwork Reduction Act of 1995. Accompanying regulations to these statutes have established "safeguards" or protection provisions to borrower information held by the regulated entities. In addition, the extensive regulatory guidelines in place for the FFELP program, the Higher Education Act of 1965, as amended, outline several borrower protection provisions.

QUERY: Should the Safeguards Rule include methods to demonstrate compliance with the Rule? For example, should a particular audit process be required for a financial institution to measure its compliance with the Rule?

RESPONSE: Financial institutions are already subject to an array of audit and review requirements and we believe that such processes will adequately address compliance with the new statute. We do not believe the statute will be served better by new, prescriptive audit requirements.

CITE: Section C. 2. Specificity of the Safeguards Rule

QUERY: Should specific steps be required to provide administrative, technical and physical safeguards for the customer records and information? And should these steps be different for each, i.e., administrative, technical, and physical? For example, should shredding of discarded paper records be required to address physical security and should employees' access to customer records be monitored to address administrative safeguards? For technical safeguards, should general standards be created for effective controls or programs or reasonable policies and procedures? In other words, should technical safeguards be monitored in a more general manner than administrative or physical safeguards? If all safeguards are more 'general', what examples or clarification of adequate safeguards should be included?

RESPONSE: The Safeguards Rule should not attempt to mandate operational, technological, or administrative aspects of the financial institution's compliance with the regulation. Financial institutions already have sufficient financial and business incentives to remain abreast of technology, operational enhancements, and other applicable changes in the marketplace. The rule should, instead, set forth a viable standard for compliance and financial institutions should be permitted maximum flexibility to design complying systems based on their expansive knowledge of the market, technology, and their own systems and operational processes. Certainly, examples provide invaluable guidance to financial institutions on how to comply with the obligations of the Act. We recommend that such examples be accompanied by a statement that clarifies that the examples are not intended to be exhaustive and that compliance with an example, to the extent applicable, constitutes compliance with the Rule.

CITE: Section C. 3. a. Anticipation of Threats or Hazards to Security or Integrity

QUERY: Should "anticipated threats and hazards" be defined? If so, how? Should the Safeguards Rule require financial institutions to anticipate threats and hazards according to particular procedures? If so, what threats and hazards should be assessed and by what procedures? Should the Safeguards Rule require financial institutions to assess threats and hazards according to particular categories ("risk categories"), such as "Risks to Physical Security," "Risks to Integrity," or "Risks in records Disposal"?

RESPONSE: The rapid pace of technology and operational processes that follow such technology make it nearly impossible to anticipate the full extent of the threats and hazards that may develop even tomorrow. However, the Rule should provide regulatory flexibility, requiring the financial institution to provide adequate safeguards but not defining precise threats or hazards to which those safeguards must respond. We believe any attempt to develop expansive lists would result in a Rule that rapidly becomes obsolete. Further, we reiterate our recommendation that the Rule be flexible rather than prescriptive with respect to safeguard processes, procedures, and systems. Financial institutions have sufficient incentives to develop effective systems and procedures and keep those systems up-to-date if the Rule provides the standards of compliance. Again, we believe that examples of threats and hazards and appropriate response procedures may prove helpful to institutions, however, we suggest text that clarifies that the examples are not intended to be exhaustive, as noted above.

QUERY: When assessing threats and hazards, should a financial institution be required to classify the value and sensitivity of the records to be protected and/or the gravity of any threats? If so, under what circumstances should such assessments be conducted in writing?

RESPONSE: Financial institutions should be required to use due care when assessing threats and hazards. However, the classification of such values and sensitivity should be left to the expertise of the financial institution and should not be prescribed in the Rule. Financial institutions already have in place standards by which they document, in writing or its equivalent, the processes, policies and procedures by which they administer their customer accounts, records, etc. We believe it would be in large part redundant to add to this recordkeeping requirement any rule specific to the Act.

QUERY: Should the Safeguards Rule require that financial institutions reassess the threats or hazards to their information security systems, and if so, at what intervals?

RESPONSE: If the rule is written with sufficient flexibility that it requires the financial institution to safeguard specific records without exception, the rule itself forces financial institutions to reassess at reasonable intervals the threats and hazards and the records to which the provisions are applicable. Additional prescriptive requirements would not add value to the statute, and might in fact provide a safe haven of non-compliance for an interval if a new threat is perceived but the reassessment is "not yet required".

QUERY: Should the Safeguards Rule define technical or other changes to an institution's information security environment that warrant reevaluation of existing safeguards?

RESPONSE: No. The Safeguards Rule should mandate general requirements but should provide maximum flexibility for the institution to develop procedures, processes and systems. Financial institutions would then routinely evaluate changes to critical systems or processes in light of the need to stay in compliance with the Rule.

QUERY: Should a financial institution be required to assess threats and hazards within a reasonable time after it knows or should know of a new or emerging threat or hazard to the security or integrity of its records?

RESPONSE: Yes. However, "reasonable" may vary according to the type of threat and the perceived risk associated with the threat. Financial institutions should be required to respond in such a "reasonable time frame" but that term should not be further defined. Financial institutions should be encouraged but not required to develop rapid response mechanisms, and advised of the wisdom of documenting the "reasonability" of the time frames prescribed within their own corporate procedures and environment.

QUERY: Should the Safeguards Rule require that the effectiveness of existing safeguards be evaluated through appropriate tests? If so, how specifically should the standards define these tests?

RESPONSE: The Safeguards Rule should require that financial institutions evaluate existing safeguards. We recommend the Safeguards Rule include examples of tests currently in use by a cross-section of the industry for use in the evaluation process. However, as noted above, such examples should be clearly noted as not exhaustive, and no prescriptive rules should be promulgated for "appropriateness". The technologies and processes for such assessments change rapidly and any such prescription is destined to be obsolete in the near future if not before publication.

QUERY: How should the Safeguards Rule protect against anticipated threats and hazards to the integrity of customer records and information? Should the protection include notifying a customer when his or her records are lost, damaged, or subjected to unauthorized access? Does insuring the integrity of customer records and information include granting customers periodic access to their records so they can monitor the accuracy of those records?

RESPONSE: The Safeguards Rule should simply require financial institutions to maintain the integrity of their customer records and information. The Rule should not prescribe the methods by which such safeguards are accomplished, nor should it prescribe the level to which customers may have access to their financial records.

CITE: Section C. 3. b. Preventing Unwarranted Access and Use

QUERY: Should the terms "unauthorized access" and "unauthorized use" as they are used in Section 501(b) of the Act be defined? If so, how? Should the Safeguards Rule require financial institutions to follow certain minimum procedures to "protect against unauthorized access to" customer records and information? If so, what procedures are most appropriate given the diverse range of financial institutions under the Commission's jurisdiction? For example, should the Safeguards Rule require that financial institutions designate a person within the institution who is responsible for preventing and detecting unauthorized access to and use of customer records and information? Are there any circumstances under which financial institutions should be required to maintain written records of their procedures for preventing unauthorized access and use?

RESPONSE: We believe that definitions of such terms may be helpful to institutions that are attempting to comply with the Act. Again, examples of such unauthorized transactions may be invaluable. However, we strongly recommend that the Rule not be prescriptive with respect to the procedures the institution uses to accomplish compliance. The Commission is charged with the governance of a wide range of financial institutions under the Act and those institutions have vastly diverse systems, procedures, processes, and operational structures, too many to anticipate that one prescriptive rule would provide meaningful guidance to even a majority of the governed population.

QUERY: Should the Safeguards Rule require that financial institutions enter into confidentiality agreements with their employees or train their employees in procedures for preventing unauthorized access to and use of customer records and information?

RESPONSE: Employee compliance with the Rule is an intrinsic part of the institution's compliance and the methods for achieving that compliance should be left to the institution to determine. Many financial institutions already have restrictive policies on employee access to or disclosure of financial information. In these cases, additional regulations would be redundant.

CITE: Section C. 3. c. Insuring Security and Confidentiality

QUERY: Does the requirement in Section 501(b) of the Act to "insure the security and confidentiality of customer records and information" mean something more than protecting against anticipated threats and hazards and unauthorized access and use? If so, what should it mean?

RESPONSE: We believe Section 501(b)(1) -- insuring the security and confidentiality -- goes hand in hand with (2), threats and hazards, and (3), unauthorized access and use to require the financial institution to exercise all due and prudent care in safeguarding customer records and information. We do not believe it is consistent with congressional intent to extend the provisions of any rule further than the statutory parameters.

QUERY: What measures should the Safeguards Rule require a financial institution to take to maintain the confidentiality and security of customer records and information it discloses?

RESPONSE: The Safeguards Rule should set the standards for compliance and should permit the financial institution to utilize the processes and procedures that best accomplish those standards. The rule should not require specific processes or procedures.

QUERY: Where applicable, should the Safeguards Rule require a financial institution that discloses customer records and information to notify the recipients of the limitations on reuse and redisclosure of the information imposed by the Privacy Rule?

RESPONSE: We do not believe that the disclosure of additional complex information to the consumer is either helpful or efficient. We believe that consumer disclosures should be limited to the options available to the consumer and the implications of those options, as applicable. Requiring overly detailed disclosures may be counterproductive to the privacy interests of consumers.

CITE: Section C. 3. d. Consideration of Other Agencies' Safeguards Standards

QUERY: Should the Commission's Safeguards Rule be similar to the proposed Interagency Guidelines and the National Credit Union Association's (NCUA) proposed Guidelines? If so, how?

RESPONSE: Yes. The Interagency Guidelines provide financial institutions the latitude to create, implement, and maintain policies, procedures, security programs, and other safeguards that are appropriate to the size and complexity of the institution and the nature and scope of its activities.

The guidelines are sufficiently broad to allow institutions that differ in size and complexity to tailor their safeguards accordingly, but contain enough detail so as to ensure all institutions maintain minimum satisfactory controls to protect their records regardless of size or complexity.

QUERY: Does the Act's requirement that the Commission issue a rule, rather than guidelines, warrant a different approach?

RESPONSE: We do not believe that a "rule" need be materially different from "guidelines". We suggest that rules may be developed within a context of flexibility and regulatory minimalism. Inasmuch as Section 504(a)(2) of the Act directs the Commission to, "Consult and coordinate with the other such agencies and authorities for the purposes of assuring, to the extent possible, that the regulations prescribed by each agency and authority are consistent and comparable with the regulations prescribed by the other such agencies and authorities" we believe that such rules should be developed to maximize the financial institutions' ability to develop efficient, effective processes that ensure compliance within the context of each institution's individual environment.

QUERY: Does the fact that the Commission does not conduct regular examination of financial institutions warrant more specific security measures?

RESPONSE: Generally, financial institutions undergo regular examinations by governing or oversight entities to test their compliance with applicable statutes and regulations. We believe rules promulgated under G-L-B will be tested adequately under these examinations.

QUERY: What, if any, features of the more general approach to safeguards taken by the SEC in its Privacy of Consumer Financial Information Final Rule are suitable for the Commission's Safeguards Rule?

RESPONSE: One of the most attractive features of the SEC's Rule is its laissez-faire approach to the adoption of policies and procedures by individual institutions. The SEC simply requires those institutions within its oversight to adopt policies and procedures to address the safeguards described in the Act. The SEC goes on to state in its Privacy of Consumer Financial Information Final Rule, "Consistent with the Act, the proposed rule further requires that the policies and procedures be reasonably designed to: (i) insure the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (iii) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

By allowing each individual institution the flexibility to develop and implement its own reasonable policies and procedures, the SEC is not forcing institutions, who likely vary in nature from one to the other, to augment their business practices to fit one mandated set of procedures.